Benchmark the Resilience of Satellite Simulators

Denise Nunes Rotondi Azevedo
National Institute for Space Research, INPE
São José dos Campos, Brasil
denise.rotondi@inpe.br

Abstract

Space projects require processes and tools that promote the required dependability degree. Satellite simulators are used to support the tasks of analysis and satellite testing, verification and operation, having themselves high dependability requirements. In addition, when these tools are used for different missions or for different phases of the same mission, they have an evolutionary characteristic and must accommodate changes preserving the dependability attributes. This work proposes the development of a benchmark to evaluate and compare simulation environments with respect to dependability and resilience, helping in choosing the most adequate product among the different alternatives and also in evaluating products across different versions and missions.

1. Introduction

Space systems are complex, operate in an environment hostile and not completely dominated by human knowledge and, besides that, once in orbit usually have a difficult, costly and almost always unfeasible maintenance. For this reason, the entire space system life cycle, since its conception to its operation, requires validation and verification processes and tools to ensure the required reliability degree.

Simulator tools are widely applied in several phases of a space mission, supporting system analysis, system verification and validation, operators training and so on. The development of a simulator is a complex task that can only be justified if the development effort is lower than the effort required for constructing the physical models. In this context, some standards for simulators development have been defined to promote portability, reusability and interoperability, facilitating their use in several phases of a space mission or across missions. For example, the Institute of Electrical and Electronics Engineers (IEEE) specified the High Level Architecture (HLA), which defines a software architecture for creating simulators from computational simulation components (simulated models) [1]. HLA is not an implementation, but rather a definition of interfaces that supports the implementation of simulators promoting reuse and interoperability. However, a major difficulty in the use of simulators in the different phases of the satellite life cycle is to certify how faithful and reliable the model is. Thus, this tests and validation tool should, itself, be also reliable, robust and fault tolerant.

The adoption of simulators development standards promotes reuse of models, but raises questions concerning the dependability of simulation environments in the presence of models developed by different teams and in different contexts. Thus, it is necessary to evaluate the simulation environments to verify if they have the ability to accommodate changes while maintaining the dependability attributes, isolating faults, insuring that new models will not affect the simulation behaviour or results. This work aims at establishing a benchmark to evaluate and compare, in a standard and systematic way, simulation environments constructed using HLA standards regarding to dependability and resilience attributes.

2. High Level Architecture

The HLA standard was developed by the American United States Department of Defence (DOD) aiming at increase the simulators interoperability and reuse, and can be defined as a software architecture for creating simulators from simulation components (models), providing a framework through which a developer can structure and describe their simulators applications.

A simulator is a hierarchy of components where in the lowest level we have a software component representing a model. When a model is HLA-conform it is known within the structure as a Federate, and an entire simulation consists of a group of Federates called Federation.

The HLA is structured in 3 main elements [2]: *(i)* Interface Specification, which defines the interfaces among Federates and between a Federate and the simulation environment, called HLA Runtime Infrastructure (RTI); (ii) Object Model Template (OMT), which defines a standard documentation for the HLA description; (iii) HLA Rules that establish what the main responsibilities of each group are. The RTI software

ISBN 978-85-7669-274-4.

should be conformed to the specification but is not part of the specification itself, it provides the necessary services to a HLA-conform simulation being compliant with the API defined by the specification [2].

The target of the proposed methodology is the HLA Standard evaluation, more specifically, the evaluation of RTI HLA in the context of Operational Satellite Simulations.

3. Resilience Benchmarking

3.1. Dependability and Resilience Concepts

According to Avizienis et al. [3], "dependability is the ability that a system has to provide a service in which you may reasonably rely" and the dependability of a system is characterized by a set of attributes: availability, readiness for correct service; reliability, continuity of correct service provision; safety, the ability to deliver service under given conditions with no catastrophic effect; integrity, absence of improper changes in the system, data or services; confidentiality, ensuring the safeguarding of information and maintainability, ease of maintenance.

In addition to the requirements of dependability it has been considered: changes and evolving concept characteristic of most systems, thus the **concept of resilience** and its various attributes began to be discussed. According to Laprie [4], the word *resilience* has been basically used as synonym to fault tolerance, not taking into account the evolutionary aspects of computing systems. Thus, a broader resilience concept should take into account the system's ability to accommodate changes. From this view, resilience is defined as "the persistence of dependability when facing changes" [4][5].

Regarding the kinds of changes in computer systems, they can be classified into three perspectives [4]: *nature*, changes can be functional, environmental or technological; *expectation*, that can be expected changes, predictable or unforeseen; *terms*, short terms changes, medium term changes (from hours to months) and long term changes (months to years).

3.2. Dependability *vs* Resilience Benchmarking

A computer system benchmark aims at obtaining meaningful and reliable systems comparisons in specific domains: processors, databases etc. Historically, the main benchmarks focus was the system performance evaluation. However, a broader definition defines benchmarking tools as standardized tools for assessing and comparing different systems within the same domain according to specific characteristics, e.g., performance, dependability, resilience, security etc. [5][6].

A dependability benchmark characterizes a computer system in the presence of faults, aiming to evaluate and compare their behaviour in terms of certain dependability attributes. We can define a dependability benchmark as a mean to assess, in a structured and standardized way, measures of dependability and performance-dependability in the presence of faults [7].

Performance benchmarks are based on two major components: the workload, which is a representation of the actual load to which the system would be subjected and a set of performance measures that characterize a benchmarked system. In the context of the dependability benchmark arise two more elements: the faultload, which is a representation of the possible faults (design, environment, etc.) to which the system could potentially be exposed and measures of dependability [5][6][8].

Although the benchmark for dependability extends the traditional benchmark concept, it still does not take into consideration the evolutionary characteristic of the systems, in regarding either to performance or to failures. In this context, the Resilience Benchmarking concept araises, whose goal is to provide generic forms of characterizing and comparing computer systems when subjected to changes, allowing the performance of resilience measures [9]. A Resilience Benchmark brings two more elements: changeloads, representing what changes are expected in terms of workload and failures, and resilience metrics. Figure 2 overviews the elements of the resilience benchmark.

In a Resilient Benchmark, the changeload should characterize, as much as possible, the changes to which the system may be subject, either functional, environmental or technological and should also incorporate predict or predictable faults in the context of changes. Metrics of resilience should observe the performance and dependability in the face of these changes and failures, including not predictable ones, i.e., they must measure the generic system capacity in addressing and accommodating these changes. As an illustration, in a simulation environment, it is possible to observe changes in the environment or models with respect to functional requirements, distribution, time

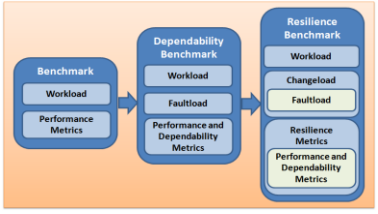

Figure 2. Components of a Resilience Benchmark. Source: adapted from Almeida e Vieira [9].

requirements, different technologies, etc.

4. Resilience Benchmarking in Satellite Simulators

Generally, satellite simulators are developed in an evolutionary way, where models may be replaced by models with a higher fidelity degree aiming to meet the needs of different phases of a space mission. Models can also be replaced by models of new equipment or subsystems. The use of standard patterns for building simulators enables the integration and use of models developed by different teams and even different organizations, promoting interoperability, reuse and portability. In a first analysis, reuse has positive impacts on the dependability attributes since it promotes quality and stability. However, this evolutionary and modular characteristic may also have negative impacts on those same attributes when we think in the constant insertion and integration of new and different models.

A resilient system should be able to accommodate changes and maintain the dependability attributes when facing changes. Satellite simulators may be subject to a set of typical changes:

a) *Among missions*: scale (number of satellites, complexity); mission objectives (spacecraft, launchers, etc.); technological (guided by evolving platforms, distribution requirements); functional (changes in models, equipment and fidelity requirements);

b) *Among the mission phases*: model addition or replacement (evolution in the fidelity requirements or changes in the goal); software-in-the-loop, hardware-in-the-loop; technological (guided by time and by the performance requirements and models complexity);

c) *Intraphase mission*: technological and systems configuration.

Therefore, the research goal is the definition of a Resilience Benchmark able to evaluate, measure and compare, in a systematic and standardized way, the dependability and resilience attributes in Operational Satellite Simulators built using infrastructure standards. The research will also provide a methodology for the process of defining this Resilience Benchmark, aiming at making this process more systematic. Figure 3 shows each process task, their interconnection and interdependence.

In general, the process of defining a benchmark starts by the definition of the domain (in the present work: the Operational Satellite Simulator using HLA infrastructure). Afterwards, for the selected domain, a set of tasks should be performed: (i) metrics, definition of the resilience attributes to be considered by the Benchmark, as well as the metrics that will be evaluated in the benchmark process; (ii) elements, definition of the architecture required to conduct the Benchmark, what includes the definition of machines, programs, operating systems, etc.; (iii) workload, definition of the workload that represents the currently use of the simulator and HLA infrastructure being evaluated, it also comprises the definition of the workload generation and instantiation; (iv) changeload, definition of the changeload that represents the potential changes that simulators and HLA infrastructure may expect, as well as the definition of changeload generations and instantiation; (v) procedure, definition of benchmark execution; (vi) validation, the proposed benchmark should be evaluated against the benchmark properties (representativeness, portability, repeatability, non-intrusiveness, scalability, simplicity). Figure 3 presents the benchmarking definition methodology.

5. Related Work

Several papers considered the dependability and robustness aspect in Satellite Simulators, analyzing and proposing fault tolerance techniques [10][11][12]. Other papers describe performance benchmark for

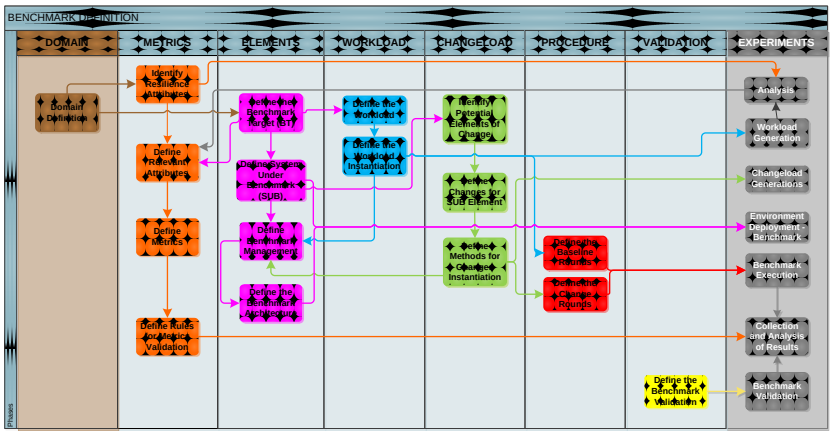

Figure 3. Benchmark Definition Methodology

RTIs developed according to the HLA standard [13] [14]. In recent years, different papers presented dependability benchmarks for many areas [6] [15] [16] [17]. Moreover proposals and definitions for resilience and resilience Benchmark [9][18] are also find.

6. Final Considerations

Simulators are widely used in space engineering, supporting analysis, testing and operation tasks, to reduce time, costs and risks in the development of satellites projects. However, simulators are themselves complex systems that are only justified if their development time consumes fewer resources than their physical counterpart while ensuring the same reliability degree. Thus, the use of development standards, the adoption of an evolutionary philosophy in the simulators construction, the use of simulators in various stages of a mission and among many satellite missions, promotes the use of these systems. However, the required dependability attributes for simulators when used as a tool to support critical systems combined to this evolutionary and changeable character, may result in difficulties in evaluation and assurance of these attributes.

The proposed work will contribute to the Space Engineering field through a Benchmark definition to evaluate and compare simulation environments regarding the attributes of dependability and resilience, assisting in selecting products from different organizations and also in assessing the reliability and stability of products developed by internal teams.

This work is innovative as it extends the dependability benchmark proposal to the resilience field considering faults and also systems changes and evolution. Besides that, the paper presents a resilience benchmark applied to the field of satellite simulators infrastructure that is an unexplored domain.

7. References

[1] B. Möller, M. Karlsson, B. Löfstrand, "Developing fault tolerant federations using HLA evolved", *In: Spring Simulation Interoperability Workshop*, 2005.

[2] High Level Architecture (HLA), IEEE 1516, 2001.

[3] A. Avizienis, J.C. Laprie, B.Randel, C. Landwehr, "Basic concepts and taxonomy of dependable and secure computing", *IEEE Transactions on Dependable and Secure Computing*, v.1, n.1, 2004, p.11-33.

[4] J.C. Laprie, "From dependability to resilience", *In: IEEE International Conference on Dependable Systems and Network (DSN'08)*, 38., 2008, Anchorage.

[5] A. Bondavalli, et al., "Research Roadmap Deliverable D3.2", *AMBER – Assessing Measuring and Benchmarking Resilience*, Funded by European Union, 2009.

[6] M. Vieira, J. Durães, H. Madeira, "Dependability benchmark for OLTP systems". In: K. Kanoun, L. Spainhower, *Dependability Benchmarking for Computer Systems*, New Jersey: John Wiley & Sons, Inc., 2008. cap. 5,p.63-90.

[7] Deliverable D13: From Resilience-Building to Resilience-Scaling Technologies: Directions, RESIST NoE, 2007.

[8] D. Costa, R. Barbosa, R. Maia, F. Moreira, "DeBERT: Dependability benchmarking of embedded real-time off-the-shelf components for space applications", In: K. Kanoun, L. Spainhower, *Dependability Benchmarking for Computer Systems*, New Jersey: John Wiley & Sons, Inc., 2008. cap. 13, p.255-283.

[9] R. Almeida, M. Vieira, "Benchmarking the resilience of self-adaptive software systems: perspectives and challenges". *In: International Symposium on Software Engineering for Adaptive and Self-managing Systems* (SEAMS '11), 6., 2011, Honolulu, New York: ACM, 2011, p.190-195.

[10] M. Eklöf, R. Ayani, F. Moradi, "Evaluation of a fault-tolerance mechanism for HLA-based distributed simulations", *In: workshop on principles of advanced and distributed simulation* (PADS '06), 20., 2006, Singapura, Washington: IEEE Computer Society, 2006, p.175-182.

[11] D. Chen, S. J. Turner, W. Cai, "A framework for robust HLA-based distributed simulations", *In: Workshop on Principles of Advanced and Distributed Simulation*, 20, 2006, Singapura. 2006.

[12] K. Fernsler, P. Koopman, "Robustness Testing of A Distributed Simulation Backplane", *In: International Symposium on Software Reliability Engineering*, 1999, 1-10

[13] P. Knight, A. Corder, R. Liedel, J. Giddens, R. Drake, C. Jenkins, P. Agarwal, "Evaluation of Runtime Infrastructure (RTI) Implementations", *In: Huntsville Simulation Conference*, 2002.

[14] L. Malinga, W. H. Le Roux, "HLA RTI Performance evaluation", *In: Siso European Simulation Interoperability Workshop*, 2009, Istambul. , P.1-6.

[15] J. Durães, M. Vieira, H. Madeira, "Dependability Benchmarking Of Web Servers", In: K. Kanoun, L. Spainhower, *Dependability Benchmarking for Computer Systems*. New Jersey: John Wiley & Sons, Inc., 2008. Cap. 6, P.91-110.

[16] J-C. Ruiz, P. Gil, P. Yuste, D. De-Andrés, "Dependability benchmarking of automotive control systems", In: K. Kanoun, L. Spainhower, *Dependability Benchmarking for Computer Systems* New Jersey: John Wiley & Sons, Inc., 2008. Cap. 7, P.111-140.

[17] D. Costa, R. Barbosa, R. Maia, F. Moreira, "Debert: Dependability Benchmarking of Embedded Real-Time Off-the-shelf Components for Space Applications", In: K. Kanoun, L. Spainhower, *Dependability Benchmarking for Computer Systems*. New Jersey: John Wiley & Sons, Inc., 2008.

[18] M. Vieira, H. Madeira, K. Sachs, S. Kounev, "Resilience Benchmark", In: K. Wolter, A. Avritzer, M. Vieira, A. Van Moorsel, *Resilience Benchmarking*, Springer Berlin / Heidelberg, 2012, 283-305.